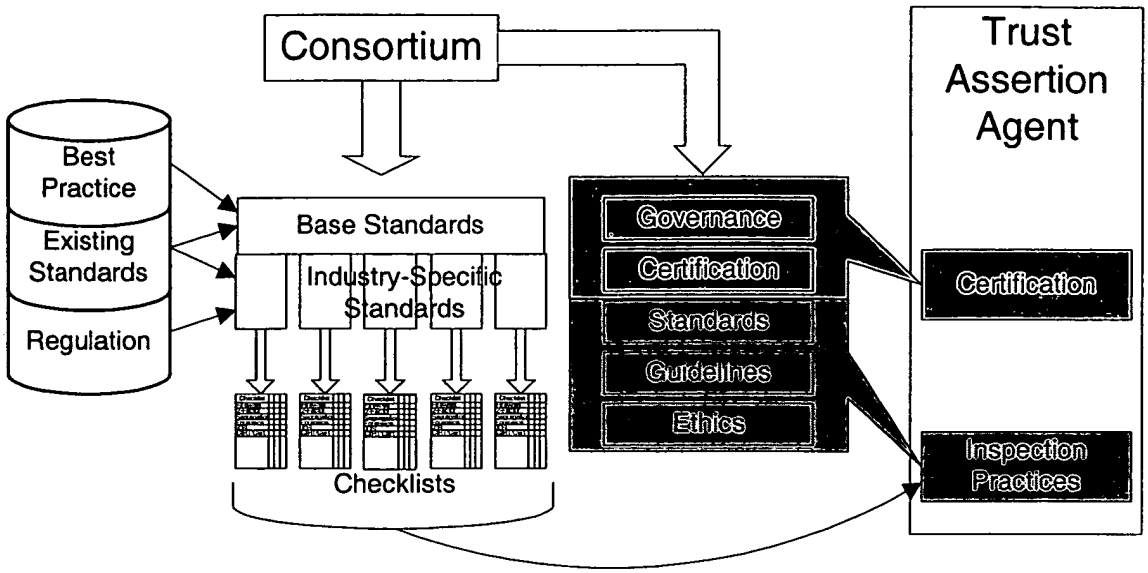

Consortium
Trust Assertion Agent
Best Practice
Existing Standards
Regulation
Base Standards
Industry-Specific Standards
Checklists
Governance
Certification
Standards
Guidelines
Ethics
Certification
Inspection Practices

FIGURE 1

FIGURE 2A

Question 45

Are servers in production DMZs hardened with an approved hardening script to within 5% of compliance?

_____ Yes _____ No

Question 46

Are servers in production DMZs hardened within an approved hardening script to within 1% of compliance?

_____ Yes _____ No

Question 47

Are production DMZ servers managed through a console protected with approved cryptography?

_____Yes _____ No

FIGURE 2B

Question 33

Are approved controls in place to ensure changes to production systems are managed and documented to within 1% of compliance?

_____Yes _____ No _____ Not Assessed

FIGURE 3

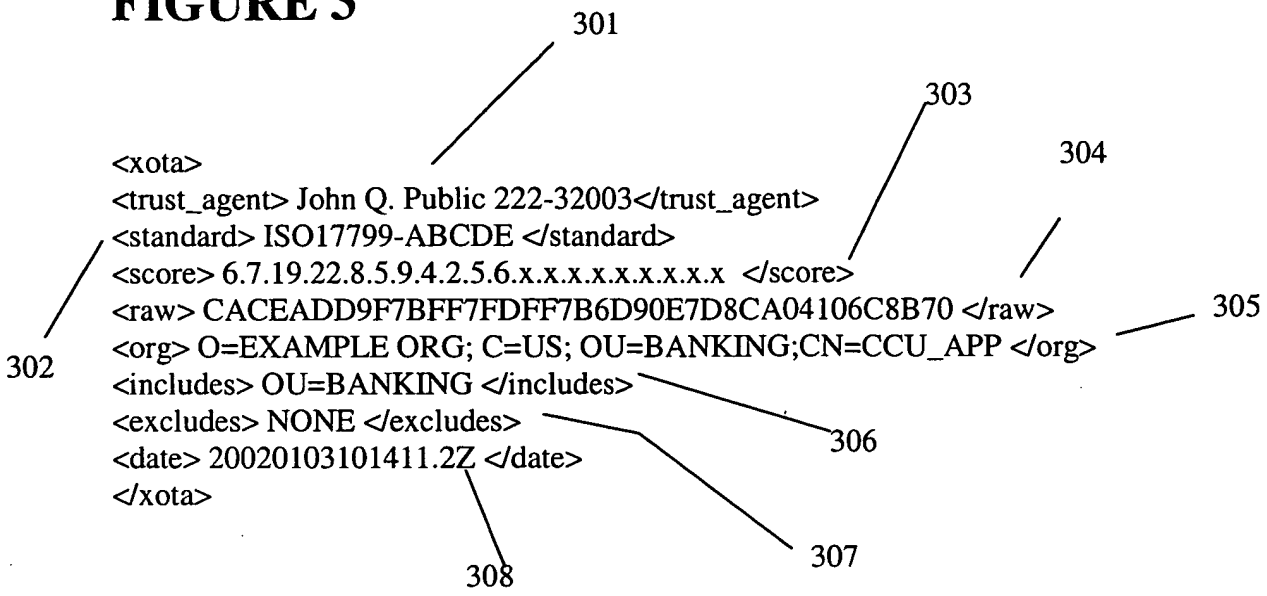

301
303
304
<xota>
<trust_agent> John Q. Public 222-32003</trust_agent>
<standard> ISO17799-ABCDE </standard>
<score> 6.7.19.22.8.5.9.4.2.5.6.x.x.x.x.x.x.x.x.x </score>
<raw> CACEADD9F7BFF7FDFF7B6D90E7D8CA04106C8B70 </raw>
305
302
<org> O=EXAMPLE ORG; C=US; OU=BANKING;CN=CCU_APP </org>
<includes> OU=BANKING </includes>
306
<excludes> NONE </excludes>
<date> 20020103101411.2Z </date>
</xota>
307
308

FIGURE 4A

11.4.17.3.1.1.7.8.6.6.X.X.X.X.X.X.X.X.X.X.X.

FIGURE 4B

Answers to Questions:

YYNNYNYNNYNY

Binary Score:

110010100101

Hex:

CA5

FIGURE 4C

Answers to Questions:
(YY = Yes, Assesed; NY = No, Assessed; NN = No, Not Assessed; YN = forbidden state)

YY YY NY NY YY NN YY NN NN YY NY YY

Binary Score:

111101011100110000110111

Hex:

F5CC37

FIGURE 4D

<xota_instream>
<standard> XYZ-12345 </standard>
<account>43925430985-2300</account>
<avgbalance> 0000031415.60 </ avgbalance >
<start> 19870103183000.0Z </start>
<end> </end>
</xota_instream>

FIGURE 5A

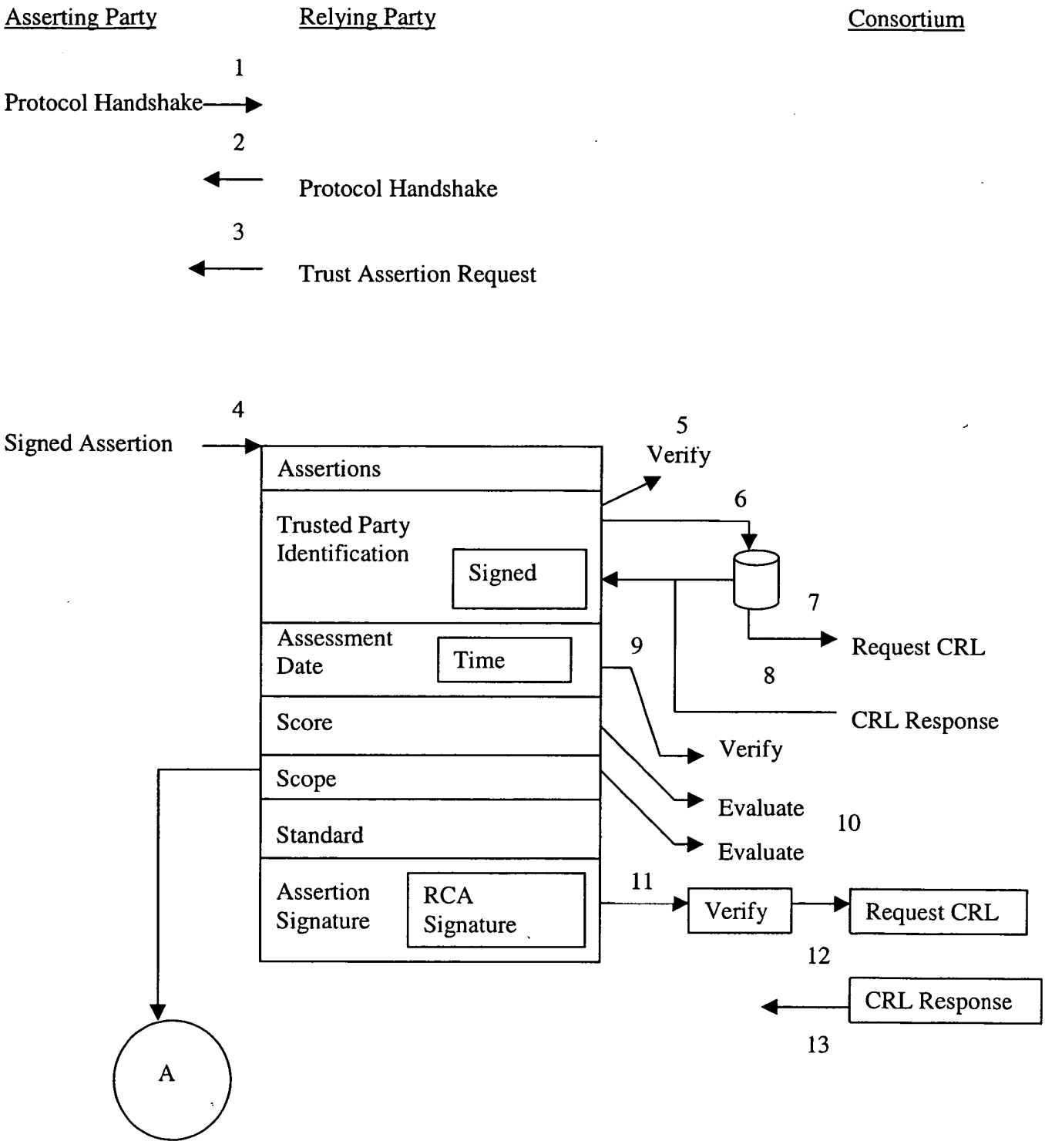

Asserting Party
Relying Party
Consortium
1
Protocol Handshake
2
Protocol Handshake
3
Trust Assertion Request
4
Signed Assertion
Assertions
Trusted Party Identification
Signed
Assessment Date
Time
Score
Scope
Standard
Assertion Signature
RCA Signature
5
Verify
6
7
Request CRL
8
CRL Response
9
Verify
Evaluate
Evaluate
10
11
Verify
Request CRL
12
CRL Response
13
A

FIGURE 5B

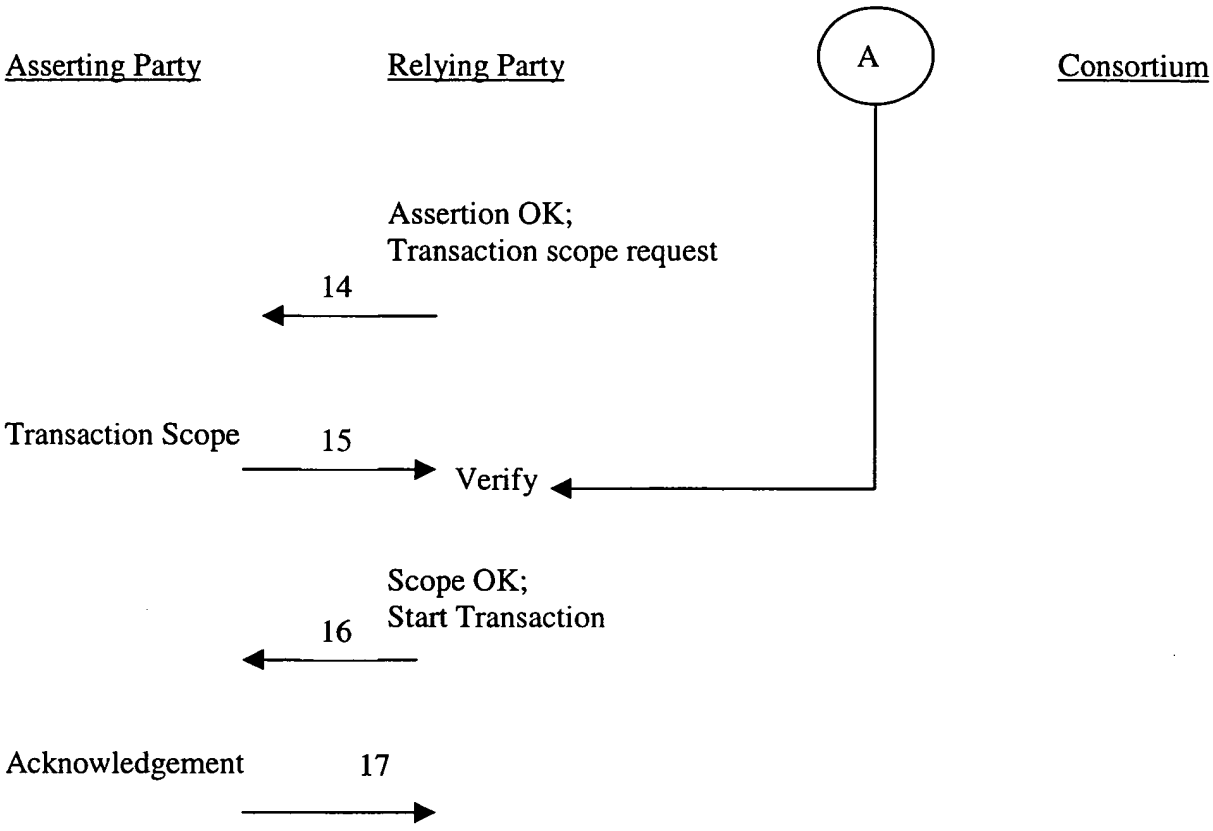

Asserting Party
Relying Party
A
Consortium
Assertion OK;
Transaction scope request
14
Transaction Scope
15
Verify
Scope OK;
Start Transaction
16
Acknowledgement
17

FIGURE 6A

```
<CTA_TEMPLATE>
<SCOPE>
 <ORG:> O=example.org; C=france; OU=abc division </ORG>
 <IN:> OU=abc division </IN:>
 <EX:> OU=abc division; CN=call center </EX:>
</SCOPE>
<STANDARD> ISO17799-ABC </STANDARD>
<SCORE>
 <CATEGORY> 3.x.x.x.4.4.x.x.x.x </CATEGORY>
 <RAW>
  <ADD> 402 </ADD>
  <DEL> 800 </DEL>
 </RAW>
</SCORE>
<ISSUER> O=example.org; C=USA; CN=CISO Office </ISSUER>
<ISSUE_DATE> 20030327233230.0Z </ISSUE_DATE>
<EXPIRE_DATE> 20030527235959.9Z </EXPIRE_DATE>
</CTA_TEMPLATE>
```

FIGURE 6B

```
S=ISO17799-ABCDE ;
C=10.17.31.30.10.9.9.11.7.11.19.15.x.x.x.x.x.x.x.x
I=3.1.1.b ;
        Yes= ;
        No=LogException ;
        No=eMailSandy ;
        Assessed= ;
        NotAssessed=LogException ;
I=3.1.1.b ;
        Yes= /usr/bin/a/scr/911.pl;
        No= ;
        Assessed= ;
        Not Assessed= ;
I=3.1.1.c ;
        Yes= ;
        No= LogException ;
        Assessed= ;
        Not Assessed= PageBob ;
.
.
.
.
.
E=ISO17799-ABCDE ;
```

FIGURE 7

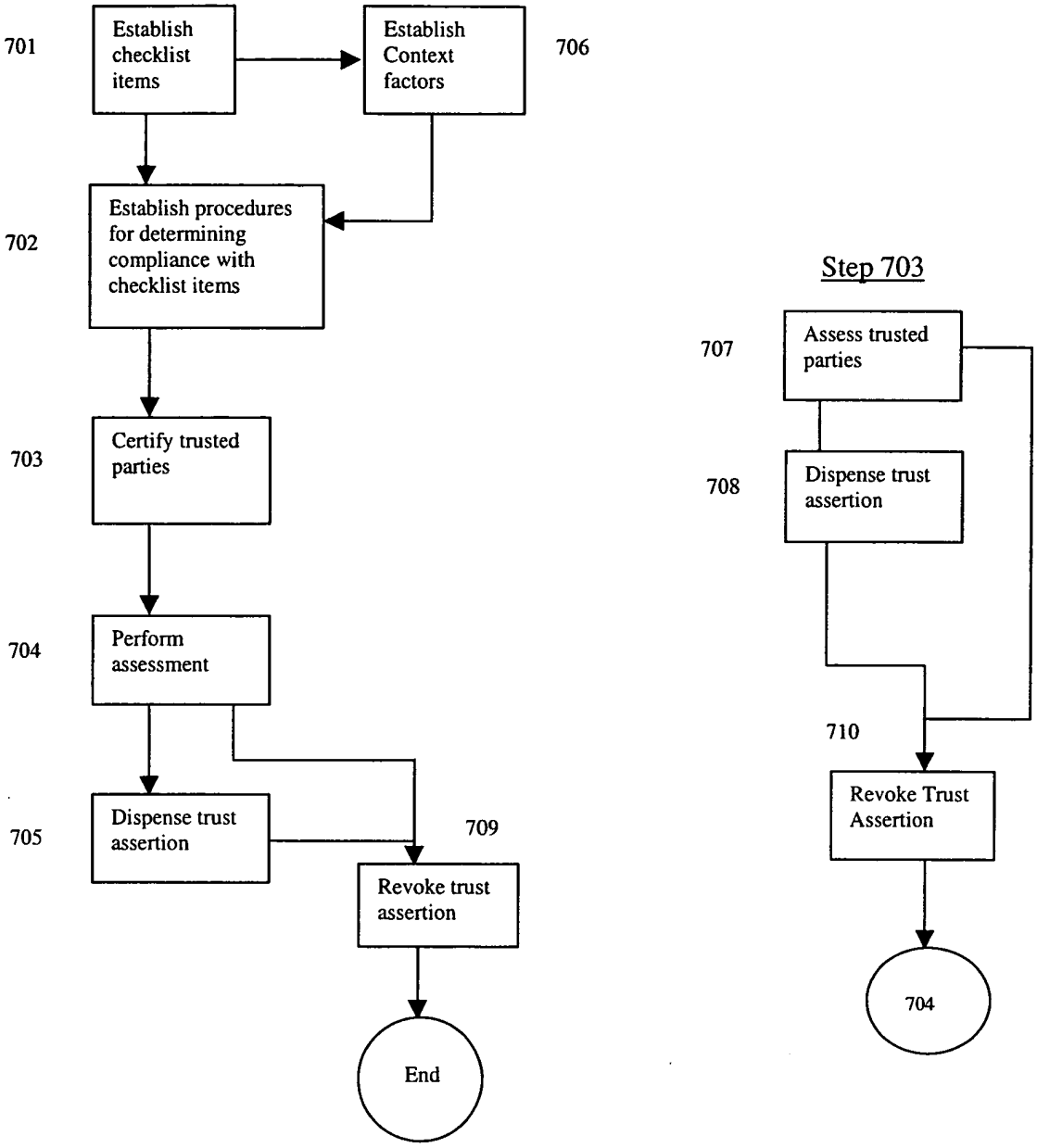

701
Establish checklist items
Establish Context factors
706
Establish procedures for determining compliance with checklist items
702
703
Certify trusted parties
704
Perform assessment
705
Dispense trust assertion
709
Revoke trust assertion
End
Step 703
707
Assess trusted parties
708
Dispense trust assertion
710
Revoke Trust Assertion
704

FIGURE 8

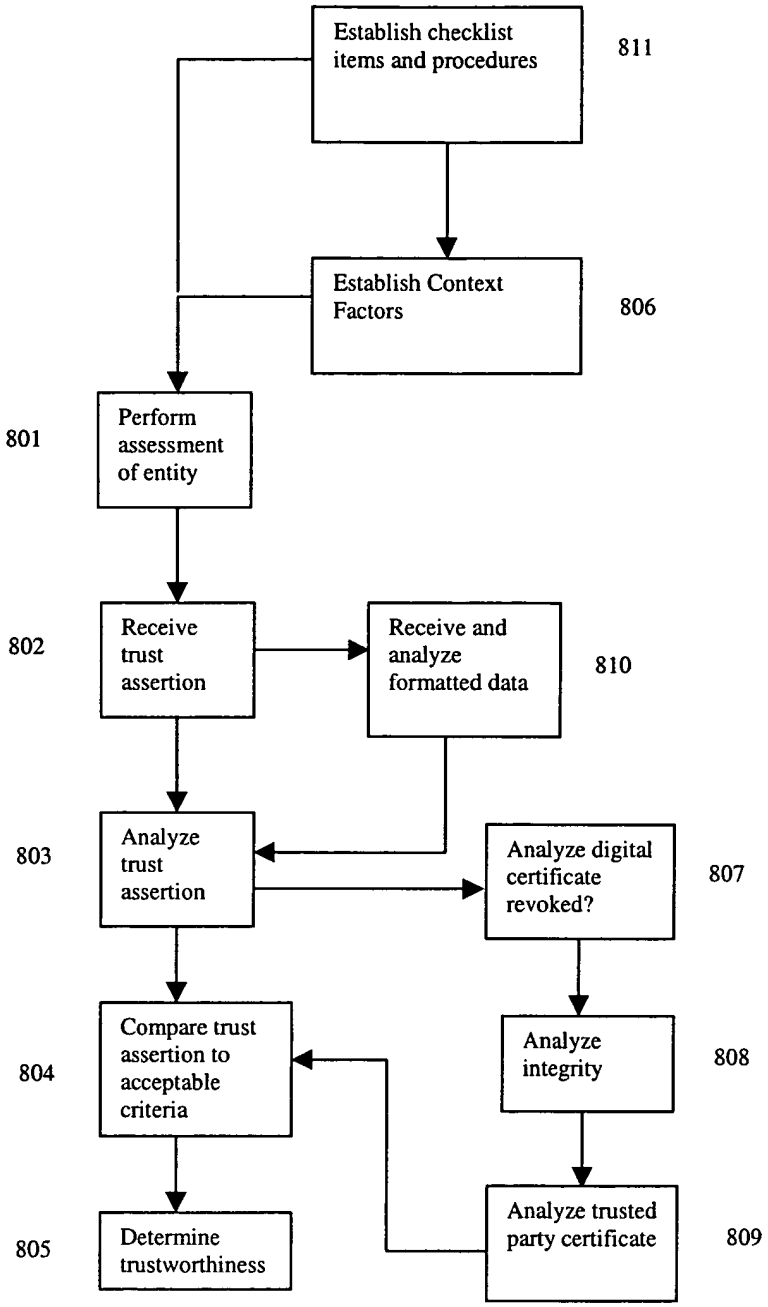

Establish checklist items and procedures
811
Establish Context Factors
806
Perform assessment of entity
801
Receive trust assertion
802
Receive and analyze formatted data
810
Analyze trust assertion
803
Analyze digital certificate revoked?
807
Compare trust assertion to acceptable criteria
804
Analyze integrity
808
Determine trustworthiness
805
Analyze trusted party certificate
809

FIGURE 9

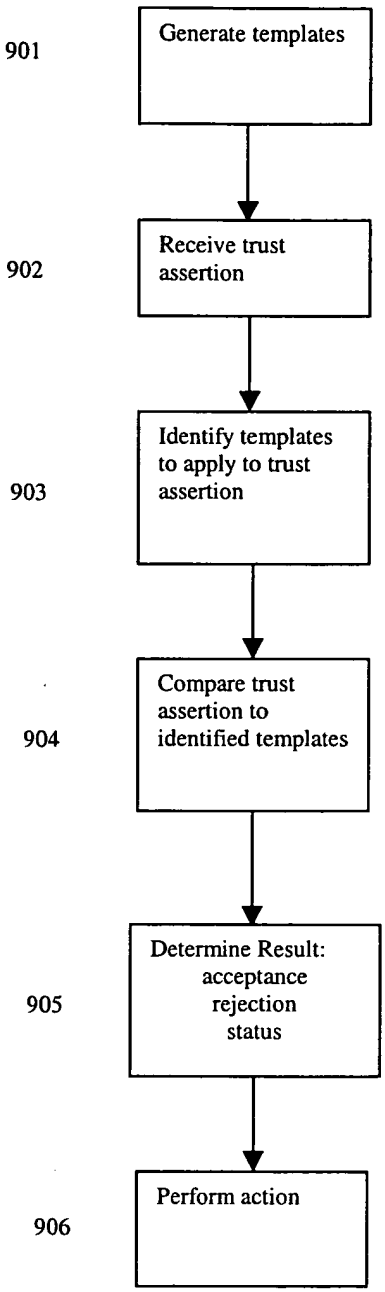

901
Generate templates
902
Receive trust assertion
903
Identify templates to apply to trust assertion
904
Compare trust assertion to identified templates
905
Determine Result:
acceptance
rejection
status
906
Perform action

FIGURE 10

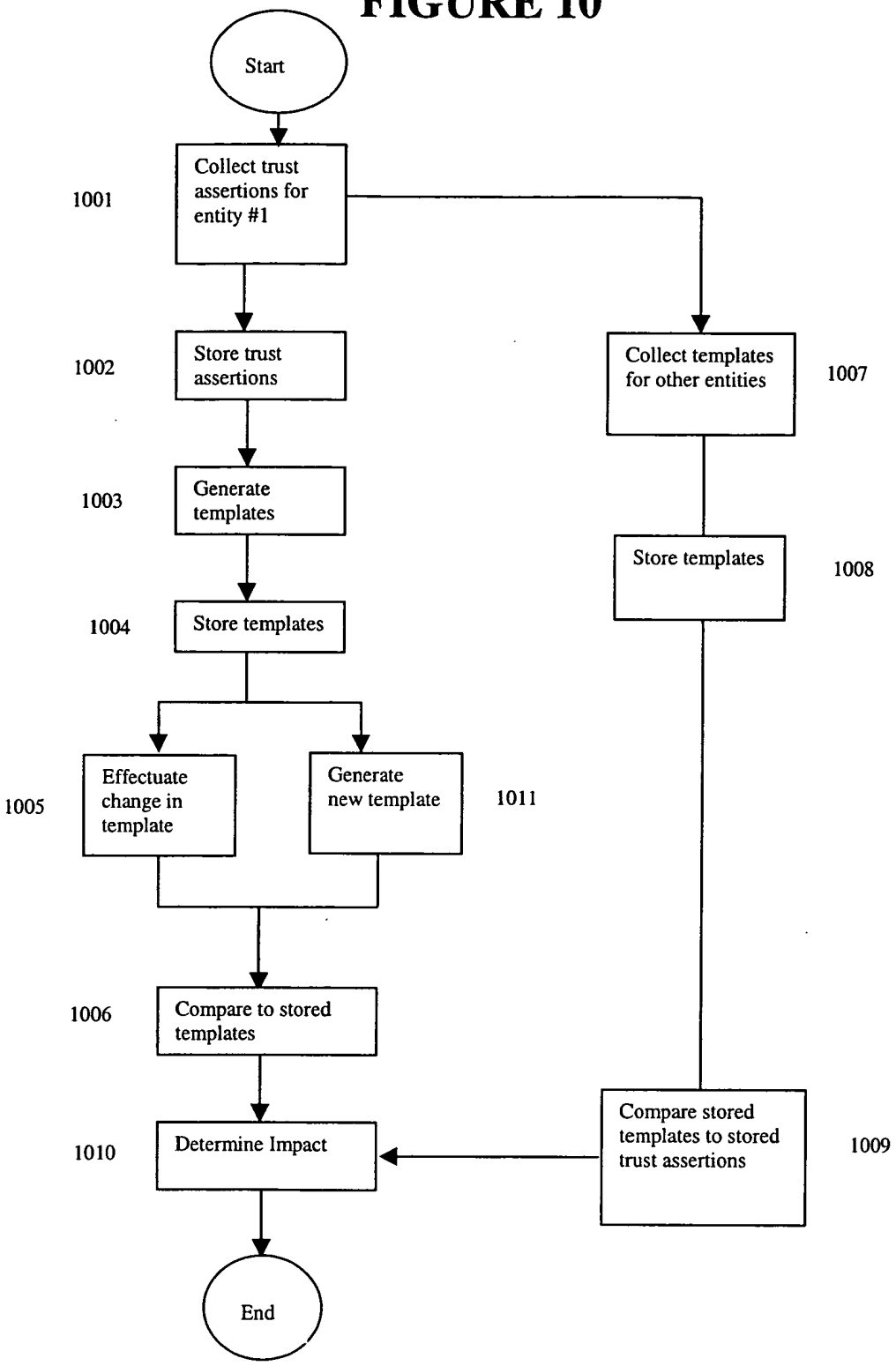

Start
Collect trust assertions for entity #1
1001
Store trust assertions
1002
Generate templates
1003
Store templates
1004
Effectuate change in template
1005
Generate new template
1011
Compare to stored templates
1006
Determine Impact
1010
End
Collect templates for other entities
1007
Store templates
1008
Compare stored templates to stored trust assertions
1009

FIGURE 11

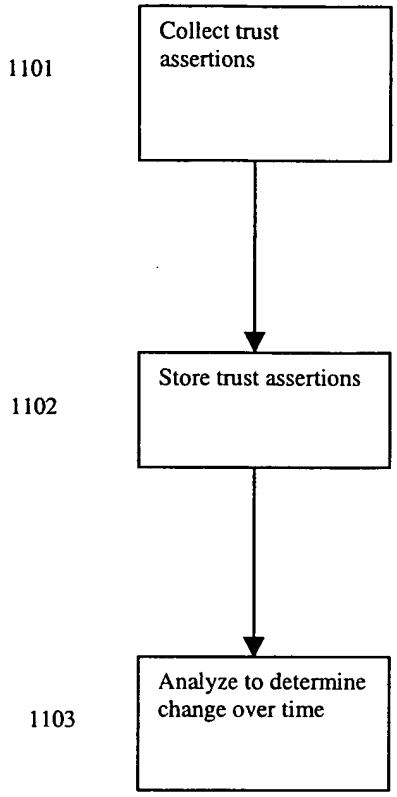

1101
Collect trust assertions
1102
Store trust assertions
1103
Analyze to determine change over time

FIGURE 12

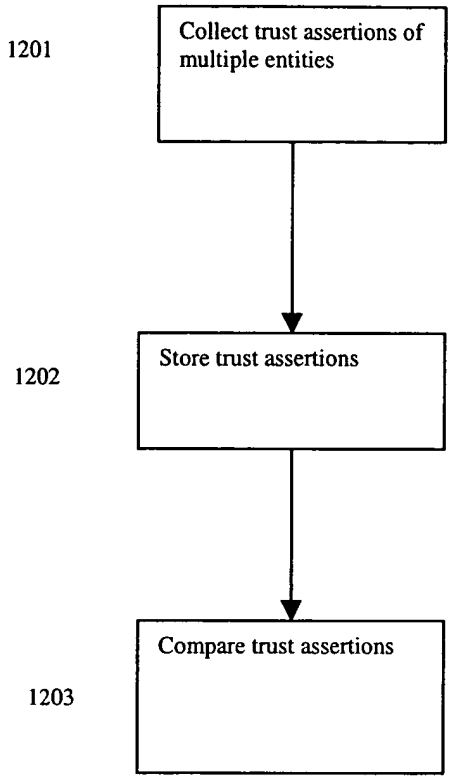
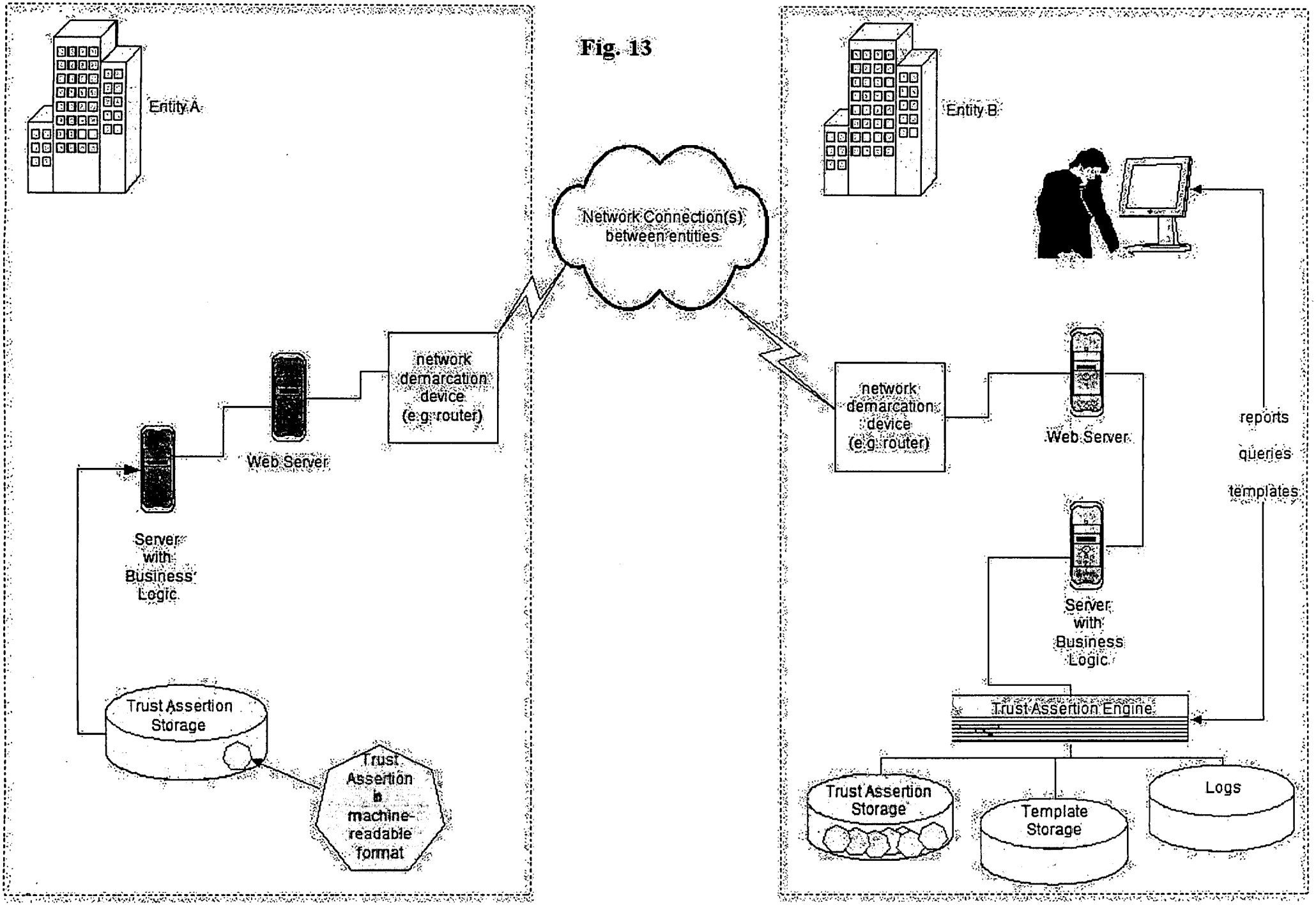

1201
Collect trust assertions of multiple entities
1202
Store trust assertions
1203
Compare trust assertions

Fig. 13


Entity A
Network Connection(s) between entities
Entity B
network demarcation device (e.g. router)
Web Server
Server with Business Logic
Trust Assertion Storage
Trust Assertion in machine-readable format
network demarcation device (e.g. router)
Web Server
reports
queries
templates
Server with Business Logic
Trust Assertion Engine
Trust Assertion Storage
Template Storage
Logs